

BEST AVAILABLE COPY

DATA DECODING METHOD AND ITS DEVICE, AUTHENTICATING METHOD, RECORDING MEDIUM, DISK PRODUCING METHOD, RECORDING METHOD AND RECORDING DEVICE

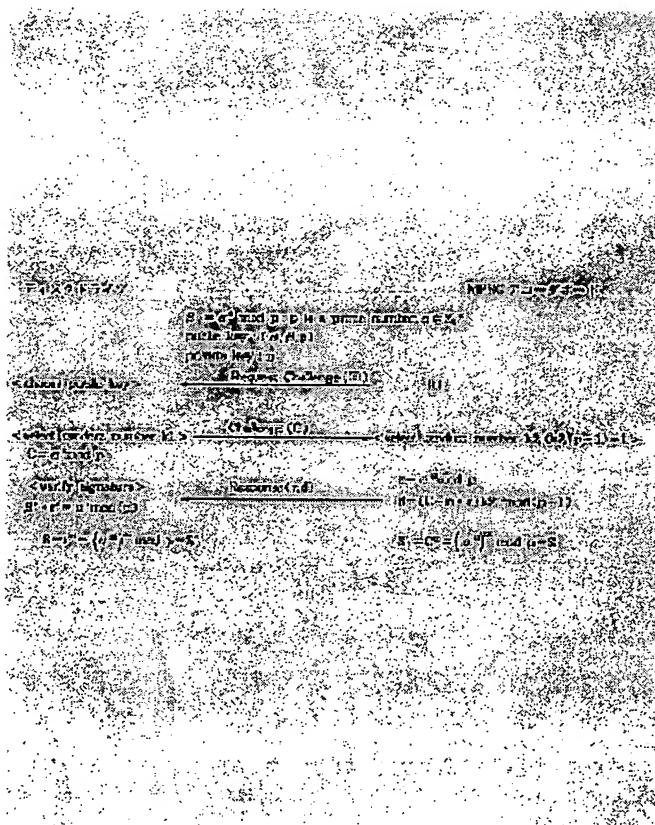
Patent number: JP10065662
Publication date: 1998-03-06
Inventor: ISHIGURO RYUJI; OSAWA YOSHITOMO
Applicant: SONY CORP
Classification:
 - international: H04L9/08; G11B20/14; H04L9/14; H04L9/32; H04N7/24
 - european:
Application number: JP19970082598 19970401
Priority number(s):

Report a data error here

Abstract of JP10065662

PROBLEM TO BE SOLVED: To surely prevent illegal copying by ciphering reproduction data which is supplied to a decoder through the use of an undecipherable cipher key.

SOLUTION: When identification data transmitted from an MPEG decoder board and a public key corresponding to its ID are judged to be effective, a disk drive calculates Challenge (C) from an expression $C = \alpha^{k1 \bmod p}$ and supplies it to the MPEG decoder board. In the expression, α and p are the public keys, p is prime number, and $k1$ is a properly selected random value. The MPEG decoder board selects the random value $k2$, calculates digital signature r and d and supplies them to the disk drive. The disk drive calculates β and γ from $\beta = r^d \bmod p$ and $\gamma = \alpha^d \bmod p$, judges whether or not the both values are equal and calculates Session key (S) in the case of being equal. In the meantime, the decoder board calculates Session key (S'). S becomes the value equal to S' and it means the same cipher key is obtained.



Data supplied from the esp@cenet database - Patent Abstracts of Japan

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 C
G 1 1 B 20/14	3 4 1	9463-5D	G 1 1 B 20/14	3 4 1 B
H 0 4 L 9/14			H 0 4 L 9/00	6 0 1 E
	9/32			6 4 1
H 0 4 N 7/24				6 7 5 A

審査請求 未請求 請求項の数23 O L (全 19 頁) 最終頁に続く

(21) 出願番号	特願平9-82598	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	平成9年(1997) 4月1日	(72) 発明者	石黒 隆二 東京都品川区北品川6丁目7番35号 ソニー株式会社内
(31) 優先権主張番号	特願平8-78647	(72) 発明者	大澤 義知 東京都品川区北品川6丁目7番35号 ソニー株式会社内
(32) 優先日	平8(1996) 4月1日	(74) 代理人	弁理士 稲本 義雄
(33) 優先権主張国	日本 (J P)		
(31) 優先権主張番号	特願平8-147272		
(32) 優先日	平8(1996) 6月10日		
(33) 優先権主張国	日本 (J P)		

(54) 【発明の名称】 データ復号方法および装置、認証方法、記録媒体、ディスク製造方法、記録方法、並びに記録装置

(57) 【要約】

【課題】 より安全な復号化方法を実現する。

【解決手段】 MPEGデコーダボードは、メモリに記憶されているIDをディスクドライブに出力する。ディスクドライブは、DVD-ROMに記憶されているキーテーブルからIDに対応する公開鍵を読み出し、この公開鍵を用いて、Challenge (C) を演算し、MPEGデコーダボードに出力する。MPEGデコーダボードは、Challenge (C) を用いて、デジタルシグニチャ r, d を演算し、ディスクドライブに出力する。ディスクドライブは、デジタルシグニチャ r, d を用いて、暗号化鍵を演算する。また、MPEGデコーダボードは、Challenge (C) を用いて、暗号化鍵を演算する。

